Aprendizaje por Refuerzo Aplicado al Etiquetado de Tráfico de Red.

Carlos A. Catania, Elina Pacini, Rodrigo Gonzalez, Jorge Guerra, Tatiana Parlanti, Luciano Robino y Eduardo Pavez

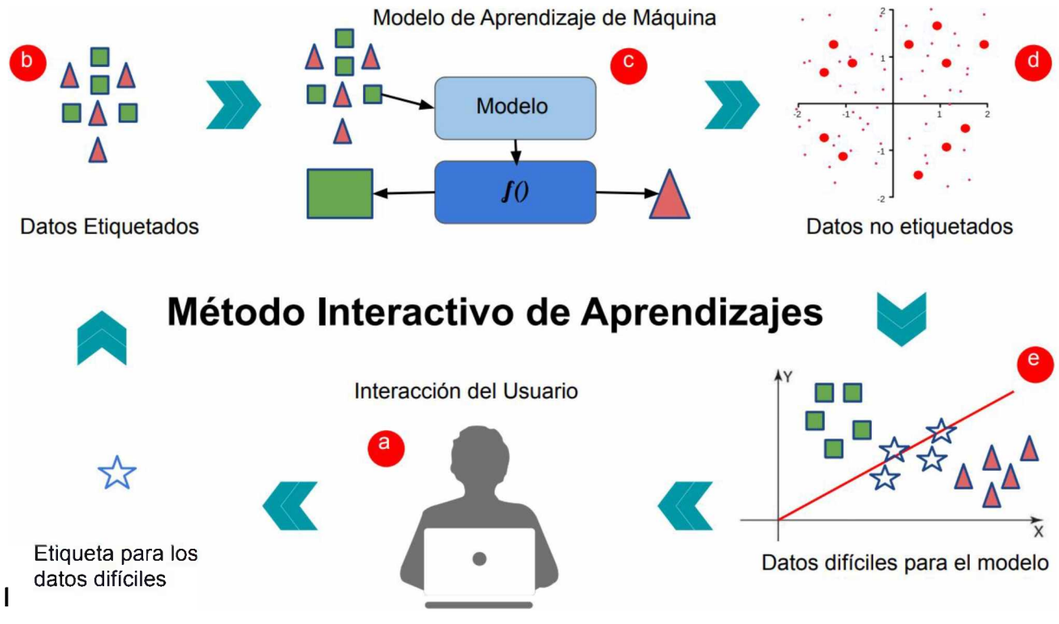
[1] Universidad Nacional de Cuyo, Facultad de Ingeniería, LABSIN
{harpo,elina.pacini,rodrigo.gonzalez,jorge.guerra,tatiana.parlanti,luciano.robino,eduardo.pavez}@ingenieria.uncuyo.edu.ar

CONTEXTO

El presente proyecto se desarrolla en el marco de Facultad de Ingeniería dentro Laboratorio de sistemas inteligentes (LABSIN). Este trabajo es parte del proyecto de investigación que dio inicio en septiembre de 2022 en el marco de los proyectos bienales de secretaria de Investigación, Internacionales y Posgrados (SIIP) de la Universidad Nacional de Cuyo.

El presente proyecto se enfoca en la aplicación de técnicas de aprendizaje por refuerzo (RL) dentro de un ciclo de Aprendizaje Activo (AL) de tal manera que permita desarrollar herramientas para facilitar el proceso de etiquetado de tráfico de red. El aprendizaje por refuerzo (RL) es un área del aprendizaje automático que se focaliza en el desarrollo de agentes inteligentes capaces de realizar acciones en un entorno a fin de maximizar una recompensa acumulada.

Normalmente, en un flujo de trabajo de AL, se aplica una política fija para decidir cuándo preguntar al usuario por el valor para la etiqueta de una instancia en particular. La política más común está basada en el concepto de incertidumbre que consiste en seleccionar aquellas trazas de tráfico que se encuentran cerca de la frontera de decisión del modelo de AA, es decir, para las cuales la política no puede decidir de manera autónoma cómo etiquetar. Sin embargo, esta política puede no resultar adecuada cuando se trabaja con grandes volúmenes de datos. Las técnicas de RL son un enfoque de reciente aplicación en el aprendizaje de una política dinámica de AL a partir de los datos. Al utilizar RL es posible aprender nuevas políticas que tengan en consideración otras recompensas como ser la experiencia o capacidad del usuario junto a aspectos distintivos del proceso de etiquetado como ser la calidad, oportunidad y relevancia, entre otros. De esta manera se evita depender de una única heurística a la hora de tomar la decisión de consultar al usuario. Esto último resulta fundamental para el desarrollo de sistemas de detección basados en técnicas de AA.



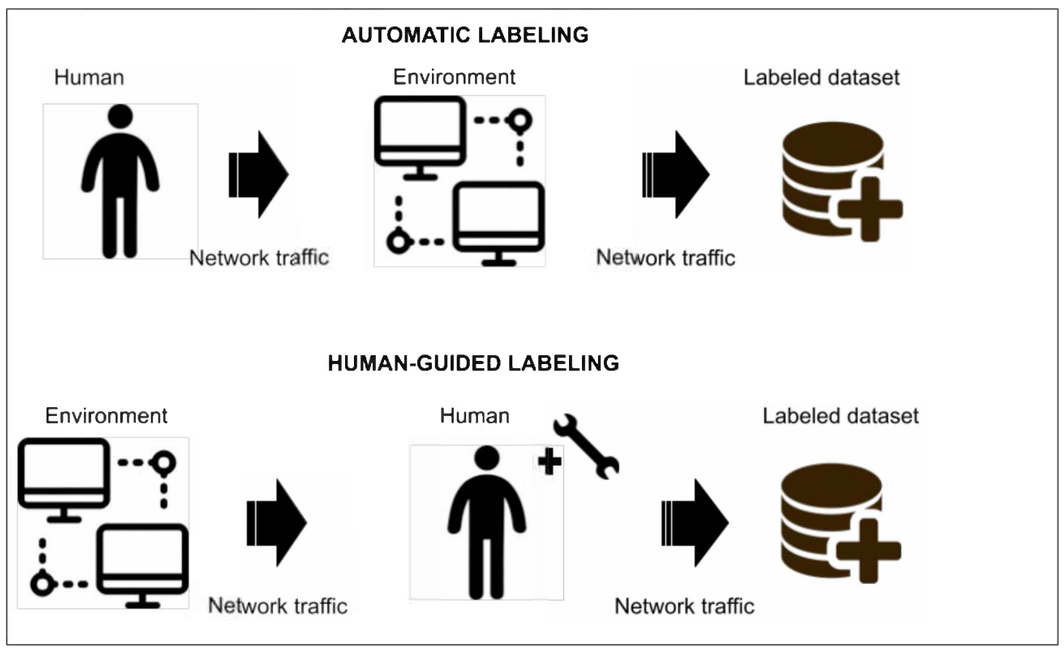


Figura 2: Diferencias entre el proceso de etiquetado automático y el etiquetado asistido. En el primero es el entorno quien etiqueta de manera automática en base a información previamente definida de los tiempos en las ventanas. Mientras que en el segundo, es el operador, quien con la ayuda de herramientas procede a un etiquetado manual.

LÍNEAS DE INVESTIGACIÓN Y DESARROLLO

El proyecto se enmarca en el área de investigación sobre la aplicación de técnicas de aprendizaje automático a la seguridad informática que se lleva a cabo en el LABSIN desde 2017.

RESULTADOS OBTENIDOS

Durante los primeros 6 meses del proyecto se completaron las actividades de:

a) Recopilación de información bibliográfica sobre el tema poniendo especial énfasis en la aplicación de técnicas de RL a problemas relacionados con la temática del etiquetado
b) Construcción de un conjunto de datos de entrada adecuado con trazas de tráfico siguiendo un enfoque automático del etiquetado automático (ver Figura 2). Dicho conjunto de datos se utilizará como referencia para la evaluación de los algoritmos basados en técnicas de AL y RL.

FORMACIÓN DE RECURSOS HUMANOS

El proyecto ha permitido la capacitación en el ámbito de la investigación a profesores y alumnos interesados en participar en un entorno académico y tecnológico innovador y a todos aquellos actores interesados en los resultados del proyecto.

Sobre la temática de este proyecto se está trabajando en:

- La tesis doctoral de Tatiana Partlanti, en el doctorado en Ciencias Informáticas de la Universidad Nacional del centro de la provincia de Buenos Aires.